COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-2766
PHONE: (213) 974-8301 FAX: (213) 626-5427

J. TYLER McCAULEY
AUDITOR-CONTROLLER

November 16, 2004

TO: Supervisor Don Knabe, Chairman
Supervisor Gloria Molina
Supervisor Yvonne B. Burke
Supervisor Zev Yaroslavsky
Supervisor Michael D. Antonovich

FROM: J. Tyler McCauley
Auditor-Controller

SUBJECT: **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY COMPLIANCE STATUS REPORT- APRIL 20, 2004 THROUGH November 12, 2004**

This is the second status report on the County's progress in implementing and complying with the HIPAA Privacy Rule. The first status report was submitted to the Board on April 19, 2004. Overall, the County continues to progress towards full compliance; while a few ongoing challenges are being addressed, the goal remains to further enhance the program by increasing its efficiency and effectiveness. To that end, the HIPAA Privacy Compliance Reviews have been effective in assessing the levels of compliance and identifying areas that require further consideration for improvement. The Chief Information Security Officer, within the Chief Information Office, is leading the effort toward complying with HIPAA's Security Rule prior to its effective date of April 20, 2005.

Los Angeles Sheriff's Department's (LASD's) Medical Services Bureau's (MSB's) Pharmacy Division

As noted in a previous Board memo submitted on December 4, 2003, LASD's Medical Services Bureau (MSB) is impacted by HIPAA since they are identified as interacting in electronic covered transactions. The State determined that its AIDS Drug Assistance Program (ADAP) is a covered health plan under HIPAA. Since MSB Pharmacy is a health care provider which now conducts covered electronic transactions, they must comply with all facets of HIPAA: Transactions & Code Sets (TCS), Privacy and Security.

On August 30, 2004, LASD submitted its HIPAA Privacy Letter of Compliance to the Chief Privacy Officer, within the Auditor-Controller, indicating that they have met all the required initial implementation mandates that included: (1) the submission of new policies and procedures; (2) training of its designated workforce; and (3) the issuance of the appropriate external business associate agreements and Interdepartmental/Intradepartmental Memorandums of Understanding (MOUs). Since LASD interfaces with the ADAP system through a State-provided web portal, the administrative and financial impact of meeting the TCS requirements were negligible. LASD is now focusing its efforts, along with the rest of the County's covered function components, to comply with the Security Rule no later than April 2005.

Medically Indigent Adult Program

As presented in the April 19, 2004 status report, certain health programs within the Department of Mental Health (DMH) and the Department of Health Services (DHS) needed analysis as possible HIPAA-covered health plans. However, based on the information currently available, we have determined otherwise. For example, the Medically Indigent Adult Program (MIAP), a State-sponsored program which provides medical and dental care to Medi-Cal ineligible indigent adults, was recently identified by other California counties and the State of California as a covered health plan under HIPAA. However, since DHS and DMH have confirmed that they no longer participate in MIAP, the issue no longer applies.

Additionally, DHS has two similar programs, the Ability-To-Pay (ATP) and the Outpatient Reduced-Cost Simplified Application (ORSA). Both programs allow the County to provide health care services to qualifying individuals at a reduced cost, or, no cost. Upon further evaluation, including guidance from County Counsel and outside counsel, we have collectively concluded that the ATP and ORSA programs are not health plans. Therefore, we do not intend to further evaluate these programs under the auspices of HIPAA.

HIPAA Privacy Compliance Reviews

During this reporting period, the Chief Privacy Officer conducted reviews of the following sites: DHS' Harbor-UCLA Medical Center (Cluster Departments 200 and 201), LAC+USC Healthcare Network (Cluster Departments 160 and 161) and Purchase Order Business Associates Program; DMH's Hollywood Mental Health Center, Edelman Mental Health Center and Arcadia Mental Health Center. The summary results from the reviews are detailed in the HIPAA Privacy Review Summary (Attachment 1).

Overall, all reviewed facilities displayed significant compliance with the HIPAA Privacy Rule. While the recent results of the HIPAA Privacy Reviews are promising, future reviews of other facilities may not result in the same outcome. The most significant discovery during the reviews was that a few HIPAA-related policies needed further review and revisions so that they would be easier to understand and execute.

During the later scheduled reviews, my Department purchased and employed automated technical vulnerabilities assessment tools to enhance the compliance review process. Those reviews included an assessment of the facilities' existing security controls and the effectiveness of those controls in protecting confidential data. A more detailed review is expected once the departments commence their mandatory risk assessment under the HIPAA Security Rule.

The number of privacy complaints submitted to either the Chief Privacy Officer or directly to the facilities remain relatively low. Despite the low number, some of the complaints identified valid and discerning privacy violations that required significant revision in departmental polices and procedures. County Counsel and the relevant departmental management are actively involved with these activities.

In the next semi-annual status report to your Board, we will include the status of the reviews from the HIPAA MOU departments including the Chief Administrative Office, Treasurer and Tax Collector, County Counsel, Internal Services Department and the Auditor-Controller. The HIPAA MOU departments are those departments that provide support services on behalf of the covered departments and are required to abide with various HIPAA privacy and security provisions. These expanded reviews will provide assurance that the terms and condition of these applicable MOUs are in full compliance and do not pose undue risk to the HIPAA-covered departments and the County.

Secure Email Update

As noted in the previous HIPAA Privacy Status Report, there is an ongoing concern regarding protected health information (PHI) being transmitted via email without sufficient safeguards. Previously conducted reviews validated the concern of enterprise-wide privacy breaches. DHS and DMH had recently approved policies that prohibited certain uses of electronic systems for processing or storing PHI until approved security controls were implemented. DHS revised its policy to permit the use of email for transmitting PHI limiting it to the DHS domain which has embedded security within its email system. However, transmitting PHI outside the DHS domain is still prohibited except for special circumstances. Per DHS' revised policy, they are required to monitor email traffic to ensure that there are no ongoing violations regarding the use of PHI within emails, especially to email domains outside of the Department. However, there has been no report submitted stating that they have initiated this requirement.

DMH's email system currently has insufficient security features to properly protect emails containing PHI. To address this issue, which the Chief Privacy Officer believes may be a HIPAA Privacy violation, DMH has opted to participate in a new secure email pilot that provides enhanced security features to their existing email system. Selected DMH staff are now capable of sending and receiving secure email even outside of the DMH domain. The secure email service protects the email and its attachments both in transit and while stored on the computer. DMH is further evaluating the system to determine if this solution will meet their strategic needs for complying with HIPAA. While

DMH is still non-compliant in this area, their ability to show sincere due diligence towards mitigating this concern should present a defensible response if it were investigated or audited by the Office of Civil Rights (OCR), the federal enforcement agency for HIPAA Privacy.

HIPAA Security

As mentioned earlier, the Chief Information Security Officer, within the Chief Information Office (CIO), is leading the countywide effort toward complying with HIPAA's Security Rule. Based on the previous HIPAA Security status reports to the Board, my department did not have a clear understanding of which tasks were expected to be completed by the deadline of April 20, 2005 and which tasks were likely to be completed after that date. On November 12, 2004, my staff met with the CIO to gain a better understanding of the overall strategy of implementing HIPAA Security for the County. As a result and to address our concerns, the CIO agreed to provide amplifying information in the upcoming Board status report for HIPAA Security which is expected to be submitted by the end of November, 2004.

Other Auditor-Controller Countywide Security Audit and Compliance Duties

On July 29, 2004, your Board approved and adopted nine (9) Information Technology (IT) and Security Policies that were presented by the Chief Information Office (CIO). These policies are now posted in Section 6 of the Board Policy Manual. On August 9, 2004, the CIO distributed a letter to all department heads informing them that these policies were effective immediately and were applicable to all departments. Specifically, Policy 6.108, "Security Auditing and Compliance", creates a new responsibility and duty for the Auditor-Controller which is to conduct security audits on all departmental information technology systems throughout the County. We estimate that there are over 150,000 computing devices and over 25,000 associated unique software application versions that would require such security audits.

This new policy, which is now in effect, presents a concern since this is an immense administrative and financial burden that was not previously planned and not currently funded. While the Auditor-Controller agrees with the intent of the policy and also believes that this is a logical duty for the Auditor-Controller, the immediate challenge is the lack of staff and resources to carry out these new duties.

To expeditiously display compliance with this policy, we have directed our Chief Privacy Officer to continue leveraging his HIPAA Privacy Reviews, in which he already conducts IT security reviews as it directly relates to HIPAA. Additional security audit and compliance reviews for non-HIPAA departments cannot be scheduled until this new initiative is properly funded. However, if there are specific and significant security concerns that could place the County at risk, we will review those systems on a priority basis.

In an effort to properly fund this new program, we plan to meet with Board IT and Health Deputies during an upcoming Audit Committee meeting to further discuss a strategy for supporting this countywide program. We will report our approach for implementing this new initiative to your Board in a future Board memo.

Summary

The County's HIPAA Privacy Program continues to increase awareness and provides a global perspective of health privacy as it relates to both health care providers and health plans within the County. Primarily due to the impact of the Privacy Rule, many staff members are more conscious of protecting their patients' health information and are actively bringing new focus to common practices that may have been the norm in the past, but could now potentially be viewed as non-compliant with HIPAA. Policy changes, such as how subpoenas are managed and how we administer special housing programs are being reviewed to better formalize these processes and to achieve a higher level of privacy protection which are not inherently HIPAA-specific issues.

The next semi-annual report is expected to be submitted in April, 2005. However, if circumstances warrant earlier reporting, we will submit a report(s) on a more frequent basis. If you have questions or require additional information, please contact me at (213) 974-8301 or have your staff contact Glen Day, the Chief Privacy Officer (HIPAA), at (213) 974-2166.

JTM:WW:GD

Attachment

c: David E. Janssen, Chief Administrative Officer
Leroy D. Baca, Sheriff
Raymond Fortner, County Counsel
Jon Fullinwider, Chief Information Officer
Dr. Thomas Garthwaite, Director, Department of Health Services
Michael J. Henry, Director, Department of Human Resources
Dave Lambertson, Director, Internal Services Department
Mark J. Saladino, Treasurer and Tax Collector
Richard Shumsky, Chief Probation Officer
Dr. Marvin Southard, Director, Department of Mental Health

HIPAA Privacy Review Discrepancy Summary Report

November 16, 2004

Facility	Severity	Discrepancy	Status
DHS' Harbor-UCLA Medical Center (Cluster Departments 200 and 201)	**Minor**	29 of Harbor's 3,685 total workforce members were not trained and were past due.	On September 23, 2004, Harbor reported that all delinquent workforce members have either been trained, transferred or terminated.
	Minor	The current Minimum Necessary Policy was deemed to be ineffective since it creates a redundant administrative burden on the hospital to re-create and redefine role-based access schemas that ensures that its workforce has the proper level of access to protected health information (PHI). Harbor was able to demonstrate that they have existing policies and procedures that meet this requirement.	**DHS is in the process of revising the policy for all of its departments. The new DHS policy is expected to be in place by November 1st, 2004.**
DHS' LAC+USC Healthcare Network (Cluster Departments 160 and 161)	**Minor**	683 (8.2%) of the Network's County paid staff were identified as not completing the training based on the data in CWTAPS. The reconciliation report was re-submitted to DHS to facilitate updating CWTAPS. Sixteen (16) USC medical students have not competed the testing and have been informed they will be removed from service unless the training is completed by August 1, 2004.	DHS is in the process of reconciling the data between CWTAPS and the Health Care Compliance System (HCCS) and has plans to migrate the HIPAA training statistics to the new learning management system (LMS) starting in October 2004. On October 14, 2004, LAC+USC reported that 99.5% of their workforce is now compliant and all but two of the medical students have been trained on HIPAA Privacy. The two who have not completed the training have been removed from service until such
	Minor	Various intake areas at the Roybal Comprehensive Health Center had PHI documents visible to patients through some of their display windows.	LAC+USC has repositioned the computers and has installed new computer privacy screens.
	Minor	Various computers at the Roybal Comprehensive Health Center that process PHI were visible to patients. If not further protected, there is likelihood that PHI may be inadvertently disclosed to patients.	LAC+USC has repositioned one of the computers and has installed new computer privacy screens.
		27 desktop computers within the same network segment were assessed using automated scanning tools. The scanned computers were assessed as being inadequately secured to prevent reasonable attempts to access PHI without authorization. A detailed vulnerability assessment report was submitted to the Network's Security Officer for a more explicit review. The following were identified as HIGH RISK concerns:	
	Major	8 computers had hard drives formatted with the File Allocation Table (FAT) file systems vs. the NT File Systems (NTFS). Hard drives formatted with FAT are less secure and present a higher risk for unauthorized access. NTFS also supports systems audit features that better support computer security forensic investigations.	**LAC+USC is converting its Windows-based file system from FAT to NTFS and will make it the technical standard for new systems prior to effective date of the Security Rule in April, 2005.**
	Major	3 computers had GUEST accounts with blank passwords enabled. This could permit easy, unauthorized access to PHI.	On October 1, 2004, LAC+USC reported that the 3 computers had the GUEST accounts disabled.
	Major	All scanned computers had multiple unauthorized access vulnerabilities due to a lack of patch management support. Many of the available patches and service packs were not installed. Some patches have been available for more than year.	**LAC+USC stated that its primary domain performs patch management and anti-virus protection on a daily basis. However, due to their lack of oversight for "grant funded" computers, they have little authority to enforce their policies and procedures. DHS is in the process of writing a new comprehensive security policy and procedure to resolve this issue prior to effective date of the Security Rule in April, 2005.**
DHS' Purchase Order Business Associate Agreements	**Minor**	DHS has identified 43 Purchase Order Business Associate Agreements (BAAs). 5 BAAs have not been signed by the relevant vendors.	On September 29, 2004, DHS reported that revised number of valid Purchase order BAAs were reduced to 42 with no agreements remaining overdue.

**** Note- Status items in BOLD are still outstanding.***

Facility	Severity	Discrepancy	Status
DMH's Hollywood Mental Health Center	Minor	1 of 73 workforce members was not trained and was past due.	Delinquent member was trained on March 25, 2004.
	Minor	Archived mental health records stored in the garage cage were not placed on palettes to mitigate against the potential of minor flooding which could destroy the records.	The Program Head reported that palettes were later obtained and installed for the archived mental health records storage.
DMH's Edmund D Edelman Westside Mental Health Center	Minor	The revised HIPAA Privacy Complaint Policy has still not been approved and signed by the DMH department head. The DMH Privacy Officer states that it has been submitted and approval is expected by June 30, 2004.	DMH approved the revised HIPAA Privacy Complaint Policy and it became effective on August 1, 2004.
	Major	The excessive storage of paper-based health records and charts continues to be a concern. The facilities are increasing their risk of unauthorized disclosure of PHI and have an increased administrative burden for managing outdated records since there is no formal policy in which to destroy outdated health records. As presented during the February 5, 2004 Preliminary HIPAA Privacy Review, the archived storage of PHI needs to be addressed such that the facilities have a clear policy and procedure in which they can appropriately destroy paper-based PHI that no longer requires maintenance.	**In February 2004, it was recommended that DMH expeditiously draft and approve a policy and procedure for destroying outdated paper-based health records and charts. To date, the policy has not been drafted.**
	Major	Various documents containing PHI, to include Progress Notes, were left unattended at cubicle 3C which was exposed to patient access.	On September 27, 2004, the Program Head reported that he resident of cubicle 3C was provided with additional HIPAA training by her supervisor and that the cubicle has since been audited for discrepancies and none were found.
	Minor	There were 26 identified computer monitors that presented PHI and were visible to patients. The Programs Heads mentioned that approximately 65 privacy screens were requested, but none were approved.	On September 27, 2004, the Program Head reported that a new request for 26 privacy screens has been submitted and is awaiting approval.
	Minor	Many of the individual Minimum Necessary Staff Forms were not documented properly. Some of the interns had different employee identification formats. There was also an inconsistency in how the fields which were deemed inapplicable were documented. Some fields were left blank, while others were marked as "None".	On September 27, 2004, the program head reported that all Minimum Necessary Staff Forms that were incorrectly documented have been corrected.

**** Note- Status items in BOLD are still outstanding.***

Facility	Severity	Discrepancy	Status
DMH's Arcadia Mental Health Center	**Minor**	The revised HIPAA Privacy Complaint Policy has still not been approved and signed by the DMH department head. The DMH Privacy Officer stated that it has been submitted for approval.	DMH approved the revised HIPAA Privacy Complaint Policy and it became effective on August 1, 2004.
	Minor	The archived storage of paper-based health records and charts were stored directly on the floor which presents an increased for records damage in the event of flooding.	On July 2, 2004, the Program Head reported that the boxed records and charts are now all placed on palettes.
		28 local computers within the same network segment were assessed using automated scanning tools. The scanned computers were assessed as being inadequately secured to prevent reasonable attempts to access PHI without authorization. A detailed vulnerability assessment report will be submitted to the DMH's Security Officer for their detailed review. The following discrepancies were identified as the HIGH RISK concerns:	
	Major	Various computers had shared accounts enabled which use shared passwords. This would also make it difficult to identify individual staff who may commit privacy breaches.	On September 27, 2004, DMH reported that it has performed a complete sweep of all machines at Arcadia Mental Health Center. All shared accounts were deleted from personal computers.
	Major	3 computers had outdated anti-virus signatures that could permit unauthorized access to PHI.	On September 27, 2004, DMH reported that it has performed a complete sweep of all machines at Arcadia Mental Health Center. All outdated anti-virus signatures were updated.
	Major	All scanned computers had multiple vulnerabilities that could permit unauthorized access due to a lack of patch management support. Many of the available patches and service packs were not installed. Some patches have been available for more than year.	On September 27, 2004, DMH reported that it has purchased a new desktop management suite. Part of the suite includes an enterprise patch management component, which DMH expects to fully deploy by April, 2005.

**** Note- Status items in BOLD are still outstanding.***